REMARKS

Reconsideration of this application is respectfully requested in view of the following remarks.

Claims 1-16 were pending in this application. In this Request for Reconsideration, Applicant has not amended, added, or canceled any claims. Accordingly, claims 1-16 will still be pending herein upon entry of this Amendment. Applicant has provided above a list of the currently pending claims for the Examiner's convenience.

In the Office Action mailed May 11, 2009, the Examiner rejected claims 1-16 under 35 U.S.C. § 103(a) as being anticipated by WO 03/001326 to Bandini et al. ("Bandini") and further in view of U.S. Publication No. 2002/0181703 to Logan et al. ("Logan"). Applicant respectfully traverses the rejections.

The present invention, as recited in the pending claims, is distinguishable over Bandini and Logan at least because (1) the digital signature is verified at the outgoing mail boundary agent rather than the receiving mail user agent, and (2) a default mail policy is applied when there is no digital signature supplied.

Verification Of Digital Signature At Outgoing Side

As described in the Abstract of the present application, embodiments of the present invention apply an email policy locally, for example, in a policy manager running on an email server of a local area network, to determine whether an outgoing email message should be allowed to be transmitted to a destination address outside the local area network, for example over the internet. The invention can use a digital signature associated with the outgoing email

message to identify the sender of the outgoing message and apply a sender-specific email policy to the message before transmitting the message. (*See, e.g.*, Abstract and page 7, lines 12-21 of the present specification.) Thus, the present invention acts on the *outgoing* side of an email communication, *before* an email message is transmitted across a wide area network.

Independent claims 1, 8, 10, and 16 recite these aspects of applying mail policies on the outgoing side of a communication. For example, independent claim 8 recites a method including "maintaining a list of computer system users and associated *sender-specific mail policies*" and "receiving a mail message intended *for further transmission*, the mail message indicating a sender thereof" (emphasis added). Likewise, independent claim 8 recites a "method of applying a sender-specific mail policy, *for use in a boundary agent of a first computer network*," "maintaining a list of users of said first computer network, and *sender-specific mail policies* associated with said users," and "receiving from a user of said first computer network a mail message intended *for further transmission over a second computer network*, the mail message indicating a sender thereof" (emphasis added). Similarly, independent claim 10 recites a *local* computer network having a mail server and *a connection to a second computer network*, wherein the mail server receives an *outgoing* mail message and, in certain circumstances, applies an associated sender-specific mail policy to the outgoing mail message. Finally, independent claim 16 recites features similar to those of claim 10, but in the context of a computer program product. Thus, each of the pending independent claims recites novel aspects related to applying sender-specific mail policies to outgoing messages.

In stark contrast, Logan merely teaches the well-known use of digital signatures to assure the identity of a sender *at the receiving mail user agent*. See, for example, paragraph [0016] of Logan, which states: "As described in the references noted above, email is managed by MTAs (Mail Transfer Agents), MDAs (Mail Delivery Agents) and MUAs (Mail User Agents). MTAs and MDAs are responsible for routing and transporting email messages while MUAs are responsible for providing an interface to users." In addition, paragraph [0025] of Logan states "At the receiving MUA, the *incoming* email may be filtered, sorted and/or identified based in part on the presence (or absence) of accompanying pledge metadata" (emphasis added).

Furthermore, in order for Logan's techniques to work, the message must have been signed using a private key obtained from a public key infrastructure. See paragraph [0027] of Logan, which states: "The integrity of a pledge as an indication of both the source and character of the associated message may be assured by 'signing' the outgoing message and pledge with a digital signature using the public key infrastructure (PKI)." See also paragraph [0032] of Logan, which states: "The digital signatures used to authenticate the message and pledge would be issued by one or more authorized certification authorities (CAs)."

In contrast, the distinguishable aspects of the present invention apply the verification of the digital signature at the *outgoing mail transfer agent* (*see, e.g.*, claim 1, which specifies "maintaining a list of computer system users and associated sender-specific mail policies; receiving a mail message intended for further transmission, the mail message indicating a sender thereof receiving a mail message intended for further transmission"). Accordingly, with the present invention, the digital signature can be verified without the need for a complex and

expensive public key infrastructure, as both the user and also the mail transfer agent can be within the same organization.

The present specification, at page 3, line 35 to page 4, line 32, describes the use of digital signatures and explains why the present invention is distinguishable over prior art similar to Logan:

> It is known in other circumstances that digital signatures can be used to identify the sender of email messages. For example, US-5,956,408 describes a method for distributing data, in which data is encrypted using a private key of the data sender, and digitally signed by the sender. The recipient decrypts the encrypted data, using a public key of the data sender, and verifies the digital signature. If the digital signature is verified, the decrypted data is enabled for use.
>
> However, as in the example given above, digital signatures are typically used only by a recipient of a message to confirm the identity of the sender or the validity of the message, after the message has been transmitted across a network.
>
> By contrast, according to an aspect of the present invention, there is provided a method of applying an email policy to determine whether a message should be allowed to be further transmitted across a network. The method according to the present invention applies a sender-dependent policy, using a digital signature to identify the sender of a message.
>
> This has the advantage that the digital signature allows the sender to be identified with a high degree of certainty, so that the sender-dependent policy can be applied correctly.

Thus, Applicant respectfully submits that the verification of a digital signature at the outgoing side of an email communication distinguishes the present invention over the prior art. Accordingly, Applicant respectfully submits that independent claims 1, 8, 10, and 16 are patentable over the prior art. In addition, Applicant respectfully submits that dependent claims

2-7, 9, and 11-15 are also patentable due at least to their dependence on an allowable base claim and for the additional features recited therein.

Default Mail Policy

Embodiments of the present invention further include the application of a default email policy for email messages that do not contain a digital signature or contain a digital signature that is not verified. (*See, e.g.*, step 72 of Figure 2 and page 8, lines 20-23 of the present specification.) The default email policy can be more restrictive than the sender-specific email policies, for example, using a longer list of keywords which mark a message as non-compliant, or regarding more filetypes as non-compliant, as described at page 8, lines 25-34 of the present specification:

> In step 82, the process applies a default email policy. The default email policy tests for specific keywords in messages, and for specific filetypes as attachments, in the same way as the sender-specific email policies described above. However, it is typically more restrictive in all respects than the sender-specific email policies applied to messages with verified digital signatures. That is, the default email policy may have a longer list of keywords which mark a message as non-compliant, or may regard more different filetypes as non-compliant.

Claims 1, 9, and 11 recite this further distinguishable feature of the present invention. Claim 1, for example, recites "if the mail message does not contain a digital signature, or does not contain a verified digital signature corresponding to the sender indicated in the mail message, applying a default mail policy to said mail message." Claims 9 and 11 recite similar features.

In contrast, Logan does not describe the use of a default mail policy in the case when there is no digital signature supplied. Indeed, Logan teaches exactly the opposite by prescribing that the unsigned mail be accepted. Paragraph [0032] of Logan states: "Unsigned mail not

containing a pledge would be handled in the usual way, but would become increasingly suspect as adoption of the anti-spam pledge mechanism becomes increasingly prevalent." Contrary to the Examiner's assertion at page 4 of the Office Action, Logan's "usual way" is not equivalent to applying any policy, let alone a default email policy – rather, Logan's "usual way" is simply to accept the mail. Logan is silent as to the application of any restrictive email policy in that situation. Thus, Logan fails to teach or suggest the present invention's methods and apparatus of applying a default email policy.

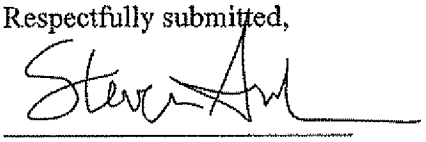
Accordingly, Applicant respectfully submits that claims 1, 9, and 11 are patentable over the prior art for at least this additional reason. In addition, Applicant respectfully submits that dependent claims 2-7 are also patentable due at least to their dependence on an allowable base claim and for the additional features recited therein.

In view of the foregoing, all of the claims in this case are believed to be in condition for allowance. Should the Examiner have any questions or determine that any further action is desirable to place this application in even better condition for issue, the Examiner is encouraged to telephone Applicant's undersigned representative at the number listed below.

PAUL, HASTINGS, JANOFSKY & WALKER LLP
875 – 15th Street, N.W.
Washington, D.C. 20005
Tel: 202-551-1700

Respectfully submitted,

Date: September 11, 2009

By: 

Steven P. Arnheim
Registration No. 43,475

SPA/dkp/hjm
Customer No. 36183